Encryption System for Supporting Hard Real-Time Distributed Testing

Kenneth G. LeSueur
Subsystem Test and Analysis Branch,
U.S. Army Redstone Technical Test Center, Huntsville, Alabama
Trent Woods and Jack Carter
ERC, Inc., Huntsville, Alabama

In the arena of distributed testing, there is a subset of applications that require hard real-time distributed interfaces to accomplish the intended mission. With the increase use of fiber optics at many installations, the ability to perform hard real-time distributed testing has become possible, that is, for all those that are not running classified real-time operations. This paper presents the design information and latency test results from a system developed at the Redstone Technical Test Center (RTTC) that enables distributed real-time classified testing applications.

Hard real-time applications are those that have a given time period to complete an operation, and if the timeline is not met, the results are invalid. To meet the timing constraints of distributed hard real-time applications, the interface or network between the separated applications must operate in a deterministic manner. The classes of hard real-time applications targeted by the new system are those that require a round-trip latency of less than 500 microseconds (μsec) and need to be encrypted by a National Security Agency (NSA)-approved class-1 encryption system prior to exiting the controlled (classified) areas. This latency time requirement includes the encryption/decryption times, speed of light over a 50 mile round-trip, and all computer/electronic interface translations.

Existing capability

Many real-time facilities/ranges utilize reflective memory systems (RM) for intersystem communications. This is especially true for hardware-in-the-loop (HWIL) facilities. RM systems are generally low latency deterministic systems that broadcast specialized memory contents to all nodes in the network, independent of operating systems and software applications. RM systems are ideally suited for real-time applications but do not have integrated class-1 encryption systems and do not extend the node rings out to 40 km, which is the target range for the RTTC solution. The RM system used for this application has a 400 ns node-to-node latency and has a 43–174 MB/s bandwidth depending on packet size (4–64 byte packets). The system can have a maximum of 256 nodes.

Most facilities/ranges that have classified operation areas and require external connectivity typically do so by using Internet Protocol (IP)-based encryption/decryption systems and networks. This approach is widely utilized for many standard interface applications but cannot meet the demanding deterministic latency requirements needed for the stated class of hard real-time target applications.

Solution

The newly developed RTTC system incorporates a high bandwidth, low latency encryption system with long-haul, single mode, fiber-optic interfaces and has plain text interfaces for RM systems, RS-422, low voltage differential signaling (LVDS), and emitter coupled logic (ECL). The system is utilized in pairs, and each pair consists of a computer equipped with a RM interface card, a KG-95 encryptor, and a custom real-time peripheral component interconnect (PCI) interface card that translates desired input formats into proper protocols for connection to the plain text side of the KG-95 encryptors. The cipher text side of the encryptor is interfaced to a fiber-optic transmitter board that translates the electronic connection to a single mode fiber-optic signal for real-time communication between the remote sites. No detailed information about the KG-95 systems is presented in this paper.

An objective of this system development is to provide a versatile connection type and protocol allowing for a wide variety of applications to seamlessly use the system. As seen in *Figure 1*, the user application can make use of the system by adding it as a node on the RM ring or providing directly

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Encryption System for Supporting Hard Real-Time Distributed Testing	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Army Redstone Technical Test Center,Subsystem Test and Analysis Branch,Huntsville,AL,35898**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**4**	

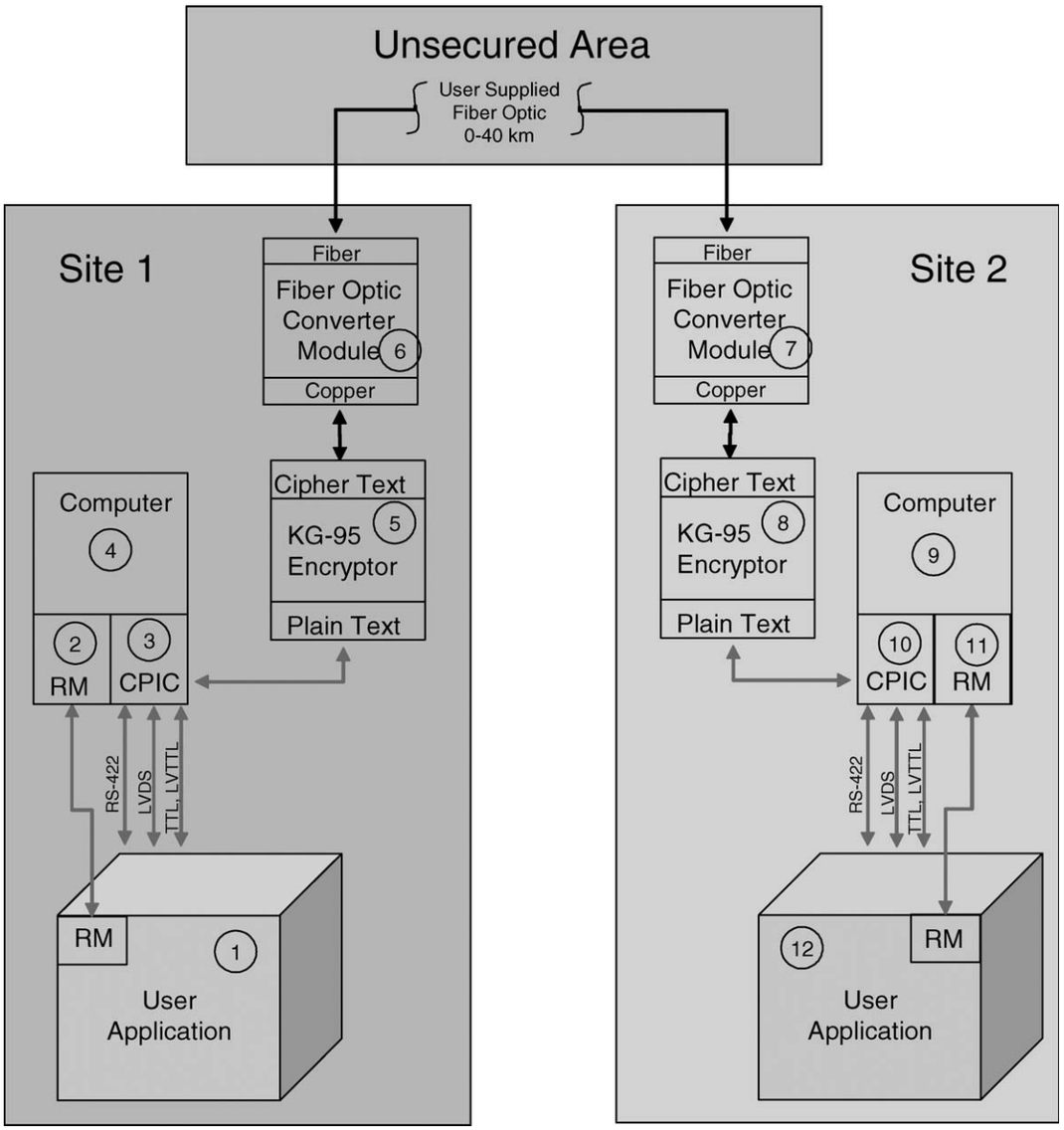

Figure 1. System block diagram

connected electrical signals from the family of standard RS-422, LVDS, or ECL interfaces. The direct electrical connections allow the user to connect test equipment, sensors, tactical hardware, or other similar equipment to the system creating a long haul encrypted extension of the electrical signal that is totally replicated on the remote end with minimal latency.

The system can currently transmit a sustained 33 Mbps and has the potential to increase to 50 Mbps with future releases of the electronics. All operation of the interface system is totally transparent to the operator and connected equipment with exception of the minimal added latency described below.

Technical description

This section will describe the functionality of each of the items in the system block diagram in *Figure 1* above. The user application box [1] in this figure is any user-supplied computer or electronic system that has an integrated RM interface card or an external

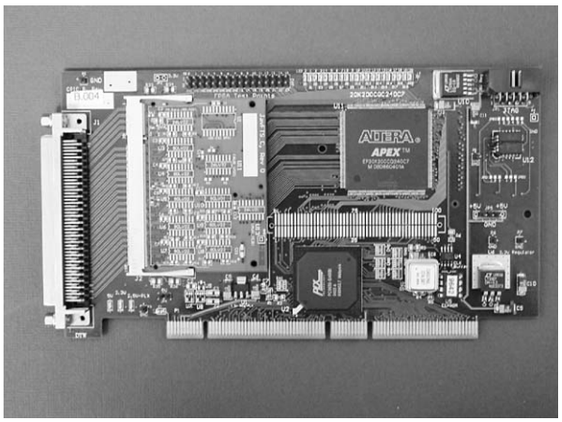

Figure 2. Configurable PCI I/O card (CPIC)

electrical interface compatible with one of the following standards: LVDS, RS-422, RS-232, transistor-transistor logic (TTL), low voltage TTL (LVTTL), positive emitter-coupled logic (PECL), ECL, and opto-isolators.

The system RM [2] card is integrated into the computer [4] via a PCI slot and provides a low latency external fiber optic interface to user applications choosing to use this interface medium.

The configurable PCI input/output (I/O) card (CPIC) [3] is integrated into the computer [4] via a PCI slot and provides the external electrical interface, translations to and from the RM, and interface to the plain text side of the KG-95 Encryptor [5] (*Figure 2*). The system currently has a sustained bandwidth limit of 33 Mbps. The system can support higher burst data rates from the data source. That is, a short duration 100 Mbps data stream could be supported. This is accomplished using the dual port random-access memory (RAM) in the CPIC. The computer [4] simply provides a housing and PCI bus for the integration of the RM and CPIC cards.

The KG-95 Encryptor [5] is a NSA type 1 certified, symmetric key encryption device that is used in the system to encrypt the incoming classified plain text data stream (represented by dashed lines, *Figure 1*) from the CPIC and provide the encrypted output data stream (represented by solid data lines, *Figure 1*) to the fiber-optic converter module [6].

The fiber-optic module converter board (FOMCB) provides an electrical interface to the KG-95 encryptor and converts the electrical signal into a single mode fiber-optic transmission source. The fiber connection between the converter modules is user supplied and can be any single mode continuous or patched fiber-optic line up to 40 km, depending on line and connection attenuation.

Items [7–12] are identical to items [1–6] providing the same functionality at the second user application location (*Figure 1*). The system is full duplex.

Test results

A test bed was developed to validate the performance of the new system and to collect system latency measurements. The RM interface was chosen for the test case. A pair of encryption systems was set up side-by-side with an 8-ft length of fiber connecting the two. A logic analyzer was connected to the appropriate signals on both systems, and test messages were generated on both sides and sent through the systems. The logic analyzer captured the critical timing parameter and the system latency is presented in *Figure 3*.

The first block of time listed in *Figure 3* is the time it takes for the CPIC to poll the dirty bit in the RM system. Currently the RM is polled at 500 kHz. The time from when the user application updates the memory to when the CPIC reads the memory change can vary between 0 and 2 μsec depending on where the update falls in the polling cycle. Test data show that the rest of the latency timeline has a variance of only 70 ns.

The second latency time block is that required for the CPIC to perform a direct memory access (DMA) transfer of the data from the RM card. The next block is the time it takes the CPIC to process and serialize the data and transmit to the encryptor. The next five timing blocks, totaling 3.95 μsec, were measured together because the encrypted data stream cannot be compared with the plain text source. The fiber-optic conversion time and the speed of light through the fiber were measured as individual components but add a very small amount of delay compared with the other parts of the system. The last timing block is the time required for the CPIC to transfer the decrypted data to the reflective memory card.

The total system latency was measured at 9.203 μsec using the 8-ft test bed fiber connection. Given the speed of light in a fiber, after approximately 1.25 miles of fiber-optics, the speed of light in the fiber will dominate the overall system latency. The fiber transmitters on the FOMCB can transmit up to 25 miles (approx 40 km). The round-trip speed of light latency through 50 miles of fiber would be approximately 1.4 *ns/ft**50 *miles**5280 *ft/mile*=370 μsec.

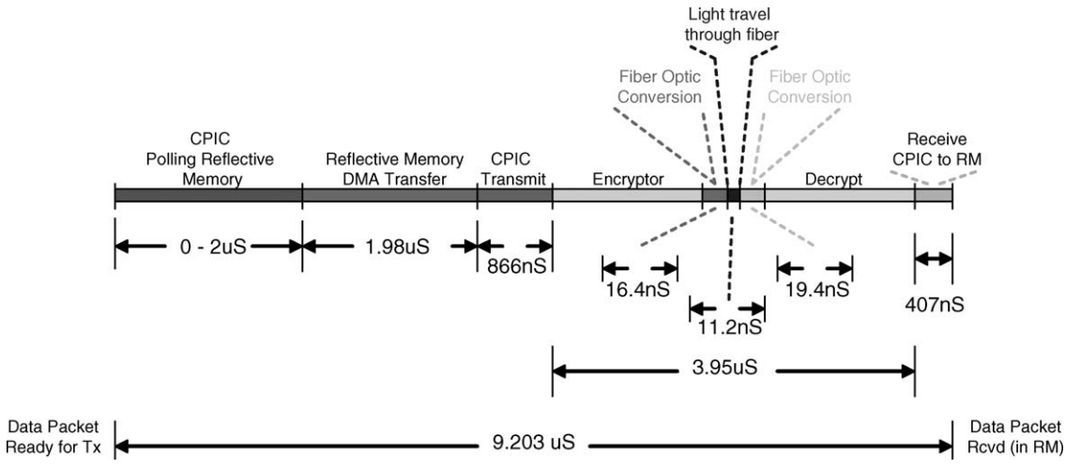

Figure 3. System latency test measurements

Adding the latency of the encryption/transmission system of 9.203 μsec for each direction, the total round-trip latency for a scenario with test sites separated by 25 miles would be 9.203 μsec+370 μsec+9.203 μsec=388.406 μsec. This fits well under our design latency budge of 500 μsec for the system. The performance of the system when operating using one of the direct electronic interfaces (RS-422, ECL, LVDS, TTL) will be similar through most of the system. The main latency driver in these modes of operation will be the time to clock in a word through the serial interface from the user application.

Conclusion

The newly developed RTTC-encrypted interface system has expanded the capability to conduct hard real-time distributed testing to include those applications that are classified. The system is extremely versatile with interfaces for RM systems and directly connected electronic interfaces. The latency of the system is low enough to maintain closed-loop performance around most demanding applications. Using the direct electronic connection configuration, the user application hardware components can be physically separated using this system, and the operator will never have to do more than turn the system on. There is no code to write, no sampling of signals, and no network configurations to make. Just hook the point-to-point fiber into the systems and start distributed testing.

RTTC has a patent pending on this system design. Hardware components have been purchased to build three complete systems for use throughout the test and evaluation community as needed. The system can also be used for unclassified activities as well. The encryptors can be bypassed and the user has a versatile, low latency tool to extend interfaces over great distances through single mode fibers. ❑

KENNETH G. LESUEUR serves as the chief technologist in the Subsystems Test & Analysis Branch at RTTC. His work & research have been concentrated in HWIL testing, distributed testing, modeling and simulation, and high performance computing. He received his master degree in computer engineering at the University of Alabama in Huntsville and is currently working on his doctoral dissertation.

JACK CARTER holds a master degree in electrical engineering from the University of Alabama in Huntsville. He is employed by ERC, Inc., as a senior engineer responsible for firmware and embedded systems development in support of ongoing test efforts at RTTC.

TRENT WOODS earned a bachelor degree in electrical engineering from Tennessee Technological University in 1986. He is a senior systems engineer at ERC, Inc., and has supported the army test and evaluation community for 20 years.